



Creative Vision for Bold Solutions

April 10, 2006

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
12th Street Lobby, TW-A325
Washington, D.C. 20554

Re: CC Docket No. 96-115, RM-11277 – Protecting Customer Proprietary Network Information

Dear Ms. Dortch:

McManis & Monsalve Associates (“MMA”) is pleased to submit comments in the above-mentioned proceeding. MMA is a management consulting firm, based in Manassas VA (on the Web at www.mcmanis-monsalve.com), dedicated to assisting government, corporate and non-profit enterprises in the United States and in Europe, in particular in the areas of data risk management, data warehousing and employee training. This FCC proceeding has a significant impact on MMA’s clients.

MMA supports the FCC exercise of its full authority granted under the Federal Communications Act (“Act”). In the adoption of the Proposed Rule, with the Act mandate, the FCC is compelled to exercise comprehensive oversight on the following four integral grounds:

I. United States Constitution; Fourth Amendment:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issues, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

The inferred precept is that of the common law definition of vicinage including the right of citizens as cell phone users/owners to be secure in their respective ambient, virtual, individual status as described by usage set forth in cell phone billing. The Proposed Rule would constitutionally protect all expressions of that living space. Conversely, failure to adopt the Proposed Rule would be tantamount to condoning constructive forms of wiretapping as trespass.

II. Technological:

Those who have purchased and/or are now purchasing, or otherwise acquiring cell phone bills or other cell phone records by current covert licit and/or illicit means over several years have had at their disposal all data conversion technologies utilized at defense agency top secret security levels for the decoding, conversion, re-encryption, and active date storage of any/all personal information accessible from cell phone records including but not limited to the physical addresses of cell phone users/owners.

III. Compliance Process:

Uses of, payments for, and operation of cell phones as a system constitute a federated, tiered, and multi-staged regulated IT environment over time and space. For compliance oversight purposes, cell phone usage lifecycles describe a phased, orthogonal marketplace subject to clandestine purchase and sale transactions by which original acquirers of cell phone records randomly resell to third parties subject to an ever expanding array of US Federal regulatory/enforcement regimes authorized to protect ever larger and vertically integrated populations of cell phone users/owners and cascades of market derivatives. Should the FCC fail to adopt the Proposed Rule, cell phone users/owners would be exposed to the above-mentioned constructive wiretapping, given the array of current commercially available data storage and conversion technologies accessible to any cell phone records acquirer. Should ongoing criminal activity be entailed in the acquisition and conversion of cell phone records, otherwise the subject of the Proposed Rulemaking, failure to adopt the Proposed Rule would avoid basic due process issues inherent in current cell phone records exposures; reciprocally, cell phone records acquirers, may in some instances, have thus far escaped applications of criminal codes for lack of "closure at the gate" of cell phone user/owner information. A compelling national interest would be realized in adoption of the Proposed Rule.

IV. Relationships Between Domestic and International Security:

Compelling adoption of the Proposed Rule on grounds of systematic integration globalizing its application are the combined effects, domestic and international, of the expected early 2007 passage of the Data Accountability and Trust Act, and of the proposed pan-EU harmonization of the EU Data Retention Directive.

In regard to the former, the House Energy and Commerce Committee have unanimously approved stringent regulations for data brokerage, precluding transactions of any kind without the knowledge and actual permission of the original user/owner of the subject information. In regard to the latter, data access limitations, preclusion of data mining, data storage systems segregation, and the grant of independent judicial scrutiny of specific data access, introduce operational parallels to the Proposed Rule.

Within the European Union, the Data Retention Directive is the subject of implementation planning by the EU Working Party ("WP"), the body of representatives of the national data protection agency advising the European Commission, which has recently issued a new "Opinion" on the implementation of the EU Data Retention Directive; the Directive addresses various principles that should provide guidance to the FCC in formulating a public understanding of the global implications of the Proposed Rulemaking. Facets of the Proposed Rulemaking, including relationships among privacy, security, and independent agency oversight, are reflected in salient provisions:

- "Data minimization: The data to be retained should be kept to a minimum, and any changes to that list should be subject to a strict necessity test."
- "No data mining"
- "Judicial/ independent scrutiny of authorized access."
- "Retention purposes of providers: Providers of public electronic communication services or networks are not allowed to process data retained solely for public order purposes under the Data Retention Directive for other purposes, especially their own. "
- "System separation: In particular, the systems for storage of data for public order purposes."
- "Security measures".

We are attaching the text of the Opinion and strongly suggest that the FCC enter into a dialogue with the WP, the European Commission, and national governments on the issues addressed in the Proposed Rulemaking to profit from the substantial expertise that these bodies have assembled.

V. Conclusion:

Systematic inter-relationships among and between the above-described recommendations for adoption of the Proposed Rule state a national interest in comprehensive oversight and integrated Federal agency performance under currently mandated jurisdictions.

We would be pleased to discuss these issues further with the FCC.

Respectfully submitted,



Marco A. Monsalve, Chairman & CEO
McManis & Monsalve Associates

Anne Renouf, Ph.D., J.D.
Management Consultant

ARTICLE 29 Data Protection Working Party



**654/06/EN
WP 119**

**Opinion 3/2006
on the Directive 2006/XX/EC of the European Parliament and of the Council on the retention
of data processed in connection with the provision of public electronic communication
services and amending Directive 2002/58/EC, as adopted by the Council on 21 February 2006**

Adopted on 25 March 2006

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

**THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS
WITH REGARD TO THE PROCESSING OF PERSONAL DATA**

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

On 21 February 2006 the Council adopted Directive 2006/XX/EC on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. The European Parliament had approved the Commission proposal (COM (2005) 0438)² as amended during the negotiations with the Council and accordingly adopted a legislative resolution on 14 December 2005 (C6-0293/2005 – 2005/0182(COD)).

In its last Opinion WP 113 of 21 October 2005 on the then draft Directive, the Art. 29 Working Party had voiced its reservations since the provisions of the Directive will have far reaching consequences for all European citizens and their privacy. The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish. The Working Party recalls the considerations and concerns set out in the aforementioned Opinion which retain their validity. It is, therefore, of utmost importance that the Directive is accompanied and implemented in each Member State by measures curtailing the impact on privacy.

The Art. 29 Working Party notes that the Directive lacks some adequate and specific safeguards as to the treatment of communication data and leaves room for diverging interpretation and implementation by the Member States in this respect. However, adequate and specific safeguards are necessary to protect the vital interests of the individual as mentioned by Directive 2002/58/EC, in particular the right to confidentiality when using publicly available electronic communications services. The Working Party considers it also crucial that the provisions of the Directive are interpreted and implemented in a harmonised way to ensure that the European citizens can enjoy throughout the European Union the same level of protection.

Therefore, the Art. 29 Working Party proposes a uniform, European-wide implementation of the Directive. This approach should guarantee a harmonized application of the provisions of the Directive whilst respecting the highest level possible of protecting personal data. This should also be done with a view to reducing the considerable costs to be borne by the service providers when complying with the provisions of the Directive.

In order to transpose the provisions of the Directive in a uniform way and to comply with the requirements of Article 8 of the European Convention on Human Rights, Member States should implement adequate and specific safeguards. At least the following safeguards should be taken into account:

¹ OJ L 281, 23.11.1995, p. 31, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

² OJ C 49, 28.2.2006, p. 42.

- 1) **Purpose specification:** The data should only be retained for specific purposes. Therefore, the term “serious crime” should be clearly defined and delineated. Any further processing should be ruled out or limited stringently on the basis of specific safeguards.
- 2) **Access limitation:** The data should only be available to specifically designated law enforcement authorities where necessary for the investigation, detection, and prosecution of the offences referred to in the Directive. A list of such designated law enforcement authorities should be made public. Any retrieval of the data should be recorded and the records made available to the supervisory authority/ies in order to ensure an effective supervision.
- 3) **Data minimisation:** The data to be retained should be kept to a minimum, and any changes to that list should be subject to a strict necessity test.
- 4) **No data mining:** Investigation, detection and prosecution of the offences referred to in the Directive should not entail large-scale data-mining based on retained data, in respect of the travel and communication patterns of people unsuspected by law enforcement authorities.
- 5) **Judicial/ independent scrutiny of authorized access:** Access to data should, in principle, be duly authorised on a case by case basis by judicial authorities without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight. Where appropriate, the authorisations should specify the particular data required for the specific case at hand.
- 6) **Retention purposes of providers:** Providers of public electronic communication services or networks are not allowed to process data retained solely for public order purposes under the Data Retention Directive for other purposes, especially their own.
- 7) **System separation:** In particular, the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes.
- 8) **Security measures:** Minimum standards should be defined concerning the technical and organisational security measures to be taken by providers, specifying more in detail the general requirements of the Directive on data retention.

The Art. 29 Working Party calls on the Member States to co-ordinate the implementation of the data retention Directive into national laws in order to guarantee a harmonised approach across the European Union and to uphold the high standard of data protection provided by both Directives 1995/46/EC and 2002/58/EC.

Done at Brussels, on 25 March 2006

For the Working Party

The Chairman
Peter Schar